CHAPTER

10

CONFIGURING CERTIFICATE SERVICES

After reading this chapter and completing the exercises, you will be able to:

- Describe the components of a public key infrastructure
- Explain the public/private key encryption process
- Explain the use of certificates
- Install and configure Microsoft Certificate Server
- Issue, manage, and revoke certificates
- Remove EFS recovery keys

Windows 2000 incorporates many industry-standard methods of securing data and other network resources. You read about many of these methods, such as IP Security and remote access authentication, throughout this book. Windows 2000 also incorporates a component named **Microsoft Certificate Server (MCS)** as part of a system to help ensure the accuracy and privacy of data as it is transferred over the network.

This chapter begins with an overview of concepts such as keys and certificates and looks at how Windows 2000 implements those concepts. Following the overview, the chapter turns to the actual installation of Microsoft Certificate Server and the management of digital certificates.

Certificate Services Overview

Traditionally, security on company networks has been largely a matter of restricting access to the network to authorized users, ensuring the proper assignment of permissions to users of network resources, and if the company network connected to a public network like the Internet, making sure that a good firewall kept out all the bad guys.

Certificates and public key encryption were originally designed for use on the Internet. Encryption keys were handed out between Web servers and from Web servers to clients using certificates or cookies. These keys were used primarily to give the client some assurance that the server was a trusted source for data. However, the trends toward requiring increasing levels of security while at the same time requiring greater scalability and exposure to the Internet led to the incorporation of certificate services on many private networks.

To meet these needs, Windows 2000 implements security using a technology called **public key infrastructure (PKI)**. While its name makes it sound complicated, a PKI is really just a system of components working together to verify the identity of users who transfer data on a system and to encrypt that data if needed. In fact, PKI is still an emerging standard, so you'll likely find that many systems incorporate a rather loose version of it. You learn about the components of PKI throughout this overview and then put them to work later in the chapter.

Certificate-based security is a complicated subject, and we do our best to explain it in the most straightforward manner in this chapter. It's helpful to keep in mind that no matter how complicated the system becomes, security is basically about two things: authentication and privacy. Authentication provides a way to let users know that the information they receive is really from the person or service that they think it is from and a way to ensure that the information has not been altered in some way since it left its source. Privacy is a means of securing the data through encryption while it is en route from source to destination. This ensures that, even if the data is intercepted, those who intercept it cannot read it.

Security Keys

In its early days (and in some systems today), encryption used a single key both to encrypt and decrypt data. Sometimes this key was a server-generated numerical sequence, but it was often a simple password shared with both the encrypting and decrypting parties beforehand. In fact, this type of key is referred to as a **pre-shared key**.

While this method did work, it was wrought with security and administration problems. It required a secure method of distributing keys and a way to keep them safe. Changing the keys frequently was also necessary to ensure security, and many applications did not lend themselves easily to this endeavor.

A method of encryption called **public key encryption** addressed the shortcomings of the pre-shared key method. This method employs two separate keys—a **public key** available to everyone on a system and a **private key** kept secret and available only to the person who holds the key. PKI uses a number of public key encryption algorithms, the most common of which is the **Rivest-Shamir-Adleman (RSA) algorithm**.

The public-key system provides two capabilities:

- Users can sign data digitally so that the recipient of the data can verify the authenticity of both the sender and the data. During this process, the sender uses her own private signing key to sign the data. The signing process does not encrypt the data in any way. The recipient uses the sender's public signing key to verify the digital signature. The message is valid if the public and private signing keys correspond to one another.
- Users can also encrypt data for secure transfer. During this process, the sender uses the recipient's public key to encrypt the data, and the recipient uses her own private key to decrypt the data.

Certificates

While the public-key encryption method is highly secure, a piece is still missing. How do you know that the public key is valid? The answer to this question comes in the form of a certificate. You can think of a **certificate** as a message of authenticity associated with a public key and coming from a trusted source. It's like getting a public key notarized. Certificates allow verification of the claim that a given public key actually belongs to a given individual. This helps prevent an impersonator from using a phony key.

In Recommendation X.509, the International Telecommunications Union (ITU) defines the most widely used format for certificates. An **X.509 certificate** contains not only the public key, but also information identifying the user and the organization that issued the certificate. This information includes the certificate's serial number, validity period, issuer name, and issuer signature.

Certificate Authorities

The issuer of a certificate is called a **Certificate Authority (CA)**. The CA is any trusted source willing to verify the identities of the people to whom it issues certificates and to associate those people with certain public and private keys. Because anyone can become a CA, certificates are only as trustworthy as the CA that issues them.

A CA issues certificates in response to a request to do so and based on the CA's policy for issuance. CAs can issue certificates to end users and computers and to other CAs. A CA accepts a certificate request, verifies the requester's information according to the policy for the CA, and then uses its own private key to sign the certificate digitally. The CA then issues the certificate to the subject (end user or other CA) of the certificate.

A third party, like VeriSign, can provide a CA, or you can set up your own CA for use in your organization. Windows 2000 provides the Microsoft Certificate Server (MCS) component for setting up a CA.

There are two different classes of CAs, and each type can operate in a number of different roles. The following sections discuss the types and roles of CAs.

Classes of CAs

MCS includes two policy modules that permit two different classes of CAs: Enterprise CAs and Stand-alone CAs. The policy modules define what actions a CA can take when it receives a certificate request.

The Enterprise CA The **Enterprise CA** acts as a CA for an enterprise, so it should come as no surprise that this type of CA requires access to the Active Directory. The Active Directory does not, however, need to be installed on the same server functioning as the CA. Enterprise CAs have a number of special features:

- All users and computers in the same domain always trust the Enterprise CA.
- Users and computers can use certificates issued by an Enterprise CA to log on to Windows 2000 domains using smartcards.
- Enterprise CAs publish certificates and **Certificate Revocation Lists (CRL)** in the Active Directory so that the information is available throughout the enterprise.
- Enterprise CAs use certificate types and templates stored in the Active Directory (and discussed a bit later in the chapter) to construct new certificates.
- Enterprise CAs always approve or reject a certificate request immediately and never mark a request as pending. The CA makes the decision based on the security permissions on the security template and on permissions and group memberships in the Active Directory.

The Stand-Alone CA The **Stand-alone CA** issues certificates to users outside the enterprise and does not require Active Directory access. For example, you might use a stand-alone CA to issue certificates to Internet users who access your company's Web site. Unlike Enterprise CAs, Stand-alone CAs typically mark incoming certificate requests as pending, because the CA is not presumed to have access to the Active Directory to validate the request. Also, Stand-alone CAs generate but do not publish certificates if no Active Directory access is present—they must be distributed manually. Finally, certificates generated by Stand-alone CAs cannot be used for smartcard logons.

Roles of CAs

Each CA class, Enterprise or Stand-alone, can operate as either a root CA or a subordinate CA. A **root CA** is at the top of a CA hierarchy, and a client trusts it unconditionally. Figure 10-1 shows how all certificate chains terminate at a root CA. The root CA must sign its own certificate because no higher authority exists in the certification hierarchy. Enterprise root CAs can issue certificates to end users but are more often used to issue certificates to subordinate CAs, which in turn issue certificates to end users.

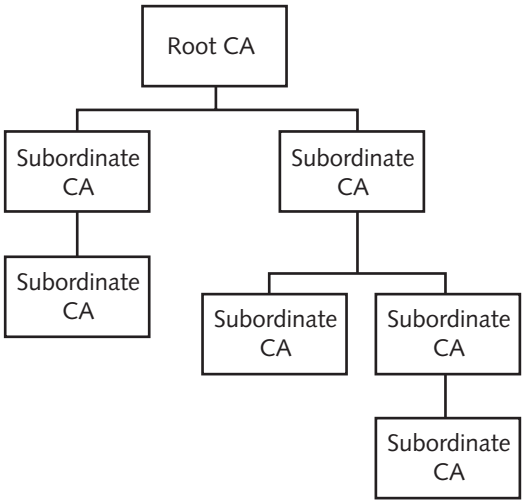

Figure 10-1 Certificate Authority hierarchy

A subordinate CA is found beneath the root CA in the CA hierarchy and maybe even under other subordinate CAs. Subordinate CAs are typically used to issue certificates to users and computers in the organization.

An organization does not need its own root CA. For example, you may establish a subordinate CA that receives certificates from another CA that belongs to a third-party company like Verisign. That way, you can let a trusted third-party take care of the security policy and use a subordinate CA mainly for convenience within your own network.

Table 10-1 lists the requirements for installing each type of CA on a Windows 2000 network.

Table 10-1 Requirements for different CA roles

Role	Requirements
Enterprise root CA	• Windows 2000 DNS Service installed • Windows 2000 Active Directory installed • Enterprise Administrator privileges on the DNS, Active Directory, and CA servers
Enterprise subordinate CA	• A parent CA, which could be an Enterprise root CA, an external commercial CA, or a Stand-alone CA • Windows 2000 DNS Service installed • Windows 2000 Active Directory installed • Enterprise Administrator privileges on the DNS, Active Directory, and CA servers
Stand-alone root CA	• Administrator privileges on the local server
Stand-alone subordinate CA	• A parent CA, which can be a Stand-alone root CA or an external CA • Administrator privileges on the local server

The Certificate Store

The **Certificate Store** is a database created during the installation of a CA. Installing certificate services on an Enterprise root CA creates the store in the Active Directory. Installing certificate services on a Stand-alone root CA creates the store on the local server. The store is a repository of certificates issued by the CA, and each store can support up to 250,000 certificates.

The Certificate Trust List

The **Certificate Trust List (CTL)** for a domain holds the set of root CAs whose certificates can be trusted. You can designate CTLs for groups, users, or an entire domain. If a CA's certificate is not on the CTL, a client responds to the untrusted certificate depending on the client's configuration. For example, you might configure a client to prompt the user for instruction on whether to allow the certificate or you might configure it to disallow the certificate automatically. Trust in root CAs can be set by policy or by managing the CTL directly. In addition to establishing a root CA as trusted, you can also set usage properties associated with the CA. If specified, these restrict the purposes for which the CA-issued certificates are valid. The Group Policy snap-in, which is beyond the scope of this book, performs all these actions.

Installing the Certificate Authority

Setting up a server as a Certificate authority is actually a pretty simple installation. As you learned from the preceding overview, planning the CAs in your network is what can get complicated. You undertake two activities to set up a CA. First, you install the MCS component on the Windows 2000 Server that will act as a CA. Second, you create an MMC console with two snap-ins, Certificates and Certificate Authority, that manage certificates. The following sections discuss both of these activities.

Installing Microsoft Certificate Server

Hands-on Project 10-1 at the end of the chapter outlines the actual steps taken to install MCS. This section provides an overview of the process. Before you actually install the MCS component, however, you need three pieces of information:

- You need to know the type of CA server you want to install: Enterprise or Stand-alone.
- You need to know the role the CA server will play in the organization: root or subordinate.
- You need to decide whether to allow users to request certificates using the optional Web interface included with MCS. This interface makes requesting certificates easier.

When you are ready to install MCS, start the Add/Remove Programs Control Panel applet and click the Add/Remove Windows Components button. You see a list of components similar to that shown in Figure 10-2.

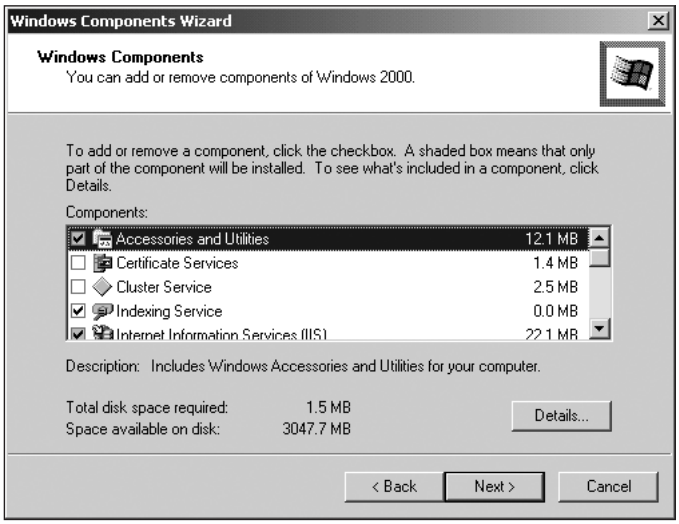

Figure 10-2 Adding Windows Components

Select the Certificate Services entry. You immediately receive a warning that after installing the component you cannot change the computer name or your current domain membership. To select specific subcomponents of the Certificate Services component to install, click the Details button to see a list of choices.

Once you select the components and click Next, the Certification Authority Type Selection page of the Window Components Wizard appears, as shown in Figure 10-3. On this page you specify your CA server's role in your organization.

If you select the Advanced option shown in Figure 10-3, you see the Public and Private Key Pair selection page shown in Figure 10-4. If you do not select the Advanced option, you skip this step altogether.

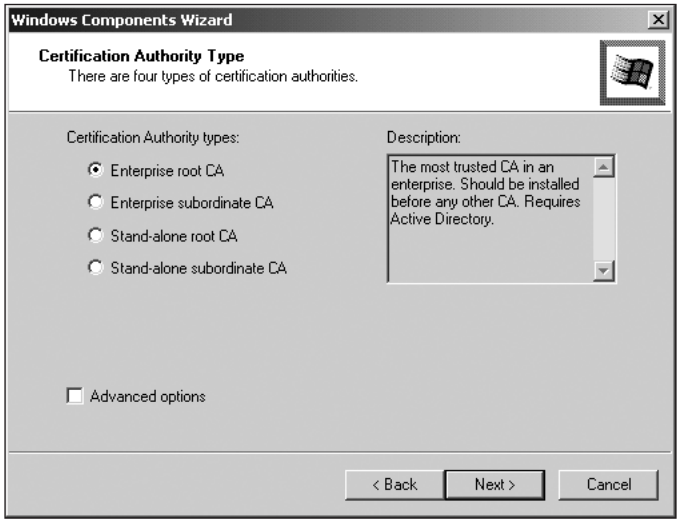

Figure 10-3 Selecting a Certification Authority type

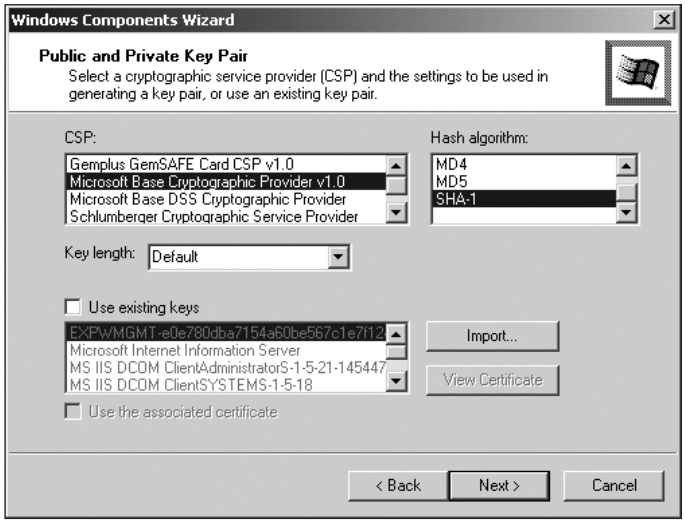

Figure 10-4 Selecting public and private key pairs

The key pair selection page lets you specify the cryptographic service providers (CSPs) you want to use. The Microsoft Base Cryptographic Provider is the standard CSP (and the only one provided with Windows 2000), but you can choose others if you have other cryptographic software or hardware installed on your network. Other options on this page include:

- *Hash Algorithm*: lists the available algorithms for computing digital signatures. SHA-1 is the default choice and the strongest algorithm available.

- *Key length*: lets you select a key length if you are generating a key pair. The default value is 1024 bits, but you can choose a value up to 4096 bits if your CSP supports it.
- *Use Existing Keys*: lets you reuse an existing key pair for the CA's key, as long as it was generated with algorithms compatible with your CSP.
- *Import button*: lets you import certificates from a PFX/PKCS#12 file (a way of distributing certificates manually).
- *View Certificate button*: shows you properties of the selected certificate.
- *Use the associated certificate*: lets you use an existing certificate if one is associated with the key pair you select and if it is compatible with your CSP.

The next step you take in the MCS setup wizard is the CA Identifying Information page, shown in Figure 10-5. This information identifies your CA to subjects requesting certificates. You must enter a CA name and an e-mail address. The rest of the information is optional but helpful. Once you enter this information and create the CA, you cannot change any of the information.

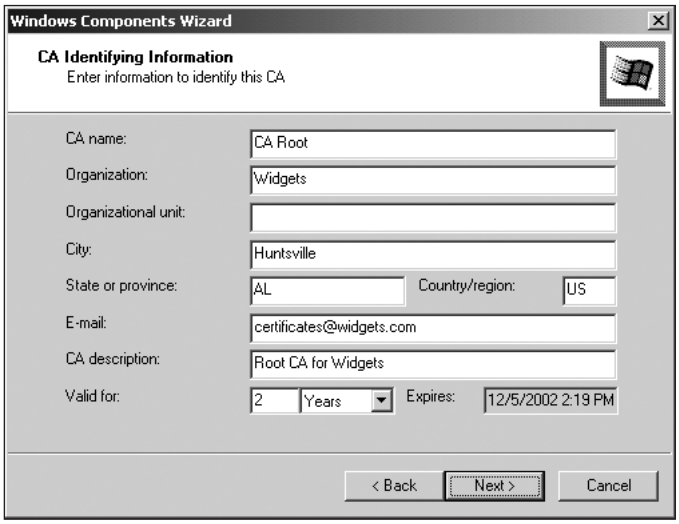

Figure 10-5 Identifying CA information

The final step in the MCS setup wizard takes you to the Data Storage Location page shown in Figure 10-6. The database configured on this page holds the certificates that the CA received from other CAs, not the certificates that the CA itself issues—those are published in the Active Directory or in another specified location. The Store configuration information in a shared folder option lets you specify a folder where the CA stores the certificates it issues. This is useful if the CA will not use Active Directory. You can use the shared folder to distribute certificates. Finally, the Preserve existing certificate database option lets you install

the CA on top of an existing CA. This is the only way you can change set-up parameters for the CA without erasing old certificates.

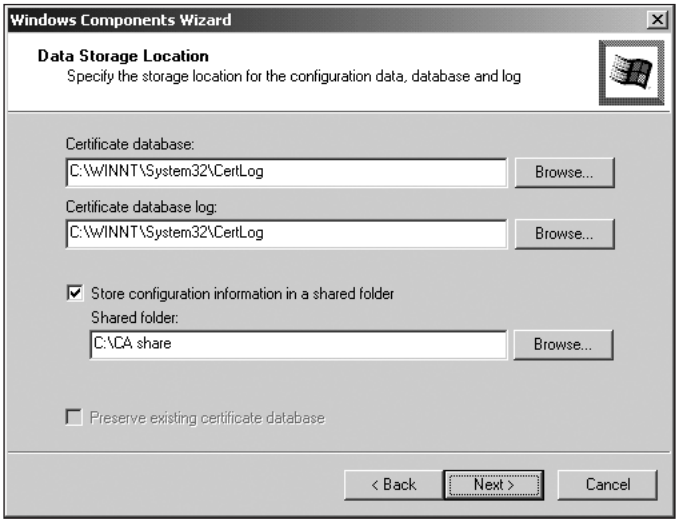

Figure 10-6 Selecting data storage locations

Installing the Certificates and Certificate Authority Snap-ins

You use two different snap-ins to manage certificates for your server. The first, named Certification Authority, manages aspects of the CA, such as policy settings, issued and revoked certificates, and pending requests. You can find this snap-in already installed in the Administrative Tools folder on your Start menu. The second snap-in, named Certificates, manages the certificates that the CA receives from other CAs. This snap-in is not installed by default; you must create a console and add the snap-in yourself. While you're creating a console for the Certificates snap-in, why not go ahead and install the Certification Authority snap-in in that console as well? That way, you can manage everything from one interface. Hands-on Project 10-2 at the end of the chapter outlines the steps for creating a new console and adding these two snap-ins to it.

Managing the Certificate Authority and Certificates

Once you install MCS and create the console with the Certification Authority and Certificates snap-ins, you are ready to start managing Certificate Services. This section covers the management tasks you undertake using the CA snap-in, shown in Figure 10-7.

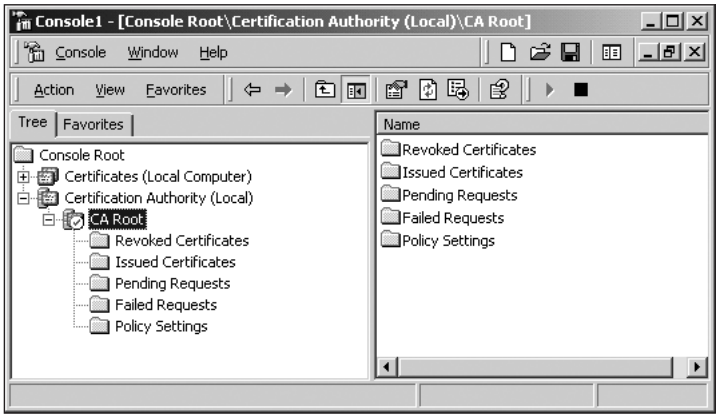

Figure 10-7 Certification Authority snap-in

Each CA node (Figure 10-7 shows only one named CA Root) holds five subfolders:

- The Revoked Certificates folder holds all certificates that the CA has ever revoked.
- The Issued Certificates folder displays the certificates the CA issued since its installation. Right-clicking a certificate allows you to revoke that certificate or open its property pages.
- The Pending Requests folder shows any requests for certificates queued on the server. An Enterprise server never has any requests queued. A Stand-alone server may. To work with pending requests, simply right-click the request and deny or approve the request right from the shortcut menu.
- The Failed Requests folder shows all failed or rejected requests.
- The Policy Settings folder shows the certificate templates available on the server. You may change the available templates by right-clicking the Policy Settings folder and using the New Certificate to issue command or the Delete command. Opening a template's property pages shows some basic information about the template, but you cannot directly edit a template.

Working with the CA

A number of commands are available for working directly with the CA. To start, you can right-click the Certification Authority container itself and use the Retarget Certification Authority command to point the snap-in at a different CA on the network. You can also access a number of commands by right-clicking the CA container itself. These include

commands for stopping and starting the CA service, backing up and restoring the service, and renewing certificates. The following sections discuss these commands.

Controlling the CA Service

By default, the CA service is configured to start each time Windows starts. You can stop and restart the service manually by right-clicking the CA container and choosing the appropriate commands. You can also stop and start the service, as well as configure whether the service starts with Windows, by using the Services item in the Computer Management snap-in. Many administrators choose not to have the service load automatically; they start the service manually during periods when they want the CA server to be able to issue certificates.

Backing Up and Restoring the CA

Right-clicking the CA container also makes commands available for backing up and restoring the CA data. The following sections discuss these commands.

Backing Up the CA Choosing the Backup CA command from the CA container's shortcut menu opens the Certification Authority Backup Wizard, which guides you through the steps for backing up the CA data. After the introductory page, you see the page shown in Figure 10-8, which lets you choose configuration settings.

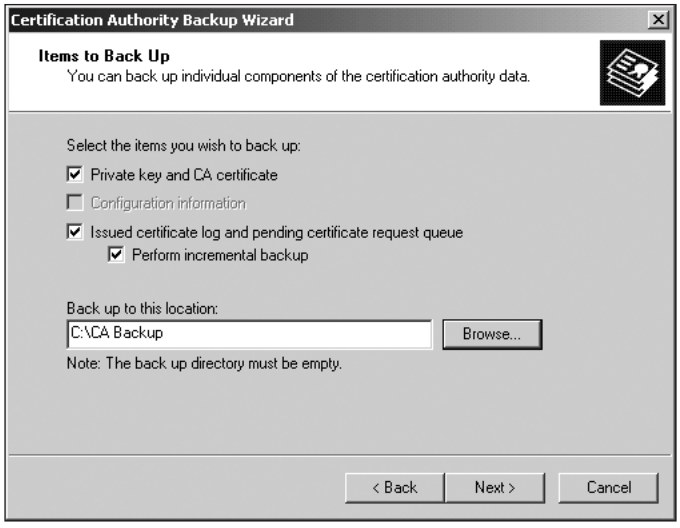

Figure 10-8 Backing up the CA

The following settings are available on this page:

- *Private key and CA certificate*: specifies that you want to back up the CA's private key and certificate. If you choose this option, the wizard asks you for a password it will use to encrypt the data.

- *Configuration information*: controls whether the configuration data for the CA is also backed up. This box is not available for Enterprise CAs, because the Active Directory stores their configuration information.
- *Issued certificate log and pending request queue*: controls whether the CAs log files for issued certificates and any pending requests are backed up. Select the Perform incremental backup option if you want to back up only those requests that changed since the last backup. Otherwise, all requests are backed up.
- *Back up to this location*: specifies the location for the backup file created. You must specify an empty directory here. You cannot store multiple backups in the same folder. The wizard creates a file named using the CA's name and the .p12 filename extension. It also creates a directory named database in the same folder.

Once you configure these settings, you are asked for the password to back up private key information if you chose that option. Then the wizard finishes and backs up the CA data.

Once the backup process is complete, you have a backup of the CA data on your hard disk. It is important, however, to include this backup in the routine backup of your server.

Restoring the CA Restoring the CA follows basically an identical, but reversed, procedure to that of backing up the CA. When you select the Restore CA command, you start a wizard that first asks you whether it can stop the CA service. You must allow it to stop the service for the restore to continue. Once the service stops, the main page of the wizard, which looks strikingly similar to the backup page shown in Figure 10-8, lets you select the items you want to restore.

Renewing a Certificate

Occasionally, you may need to renew a certificate granted to your CA. You do this by right-clicking the CA container and choosing the Renew CA Certificate command. If your CA is a subordinate CA, it requests a new certificate from its parent CA. If your CA is a root CA, it grants its own renewal request. It does this in one of two ways:

- The CA takes its existing keys and binds them to a new certificate. This is a common choice because it allows you to keep reusing existing keys for signature verification and signing. However, repeatedly using existing keys can cause the CA's Certificate Revocation List to grow quite large.
- The CA can also generate a new key pair and use it to create a new certificate. This choice is useful to keep the CRL from growing large and when you think the security of your old certificate may be compromised.

Figure 10-9 shows the dialog box that offers both these options.

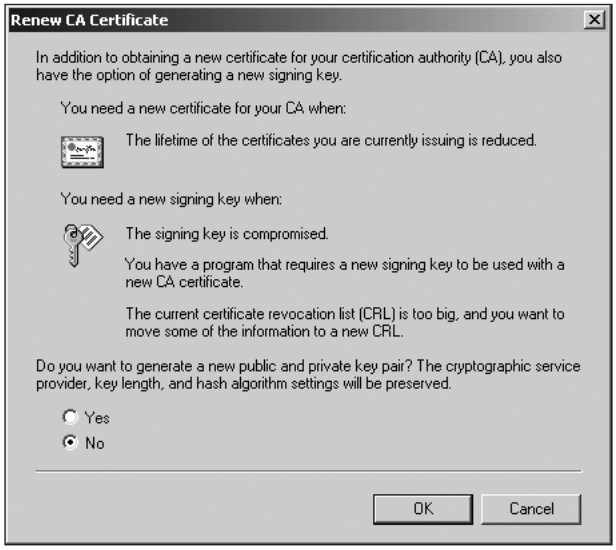

Figure 10-9 Renewing a certificate

Configuring Properties for the CA Object

In addition to using the CA container to use the commands just discussed, you can also open the property pages for the CA container to configure parameters governing the CA's behavior. The next few sections discuss each of these pages.

General Properties

The General page, shown in Figure 10-10, really only provides some information not related to configuration, such as the name and description of the CA and the current security settings. You can also use the View Certificate button to see the details of the CA's certificate.

Policy Module Properties

The Policy Module page, shown in Figure 10-11, displays the policy module currently active for the CA. Usually, this module is the default Enterprise and Stand-alone Policy Module supplied with Windows 2000. You can use the Select button if you want to use a new policy instead.

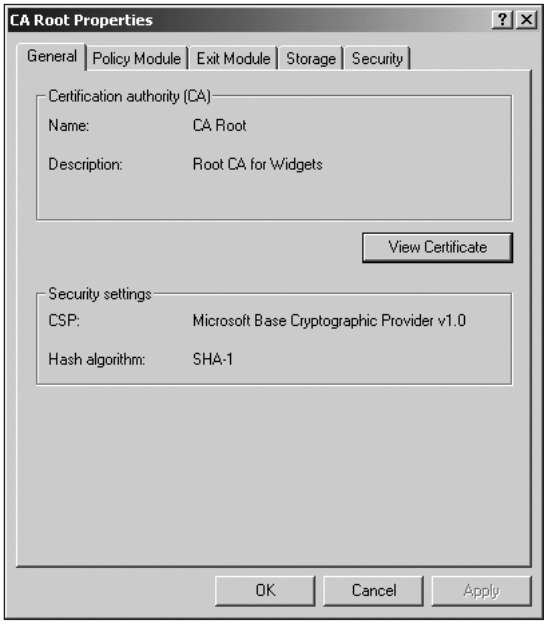

Figure 10-10 General page of CA object

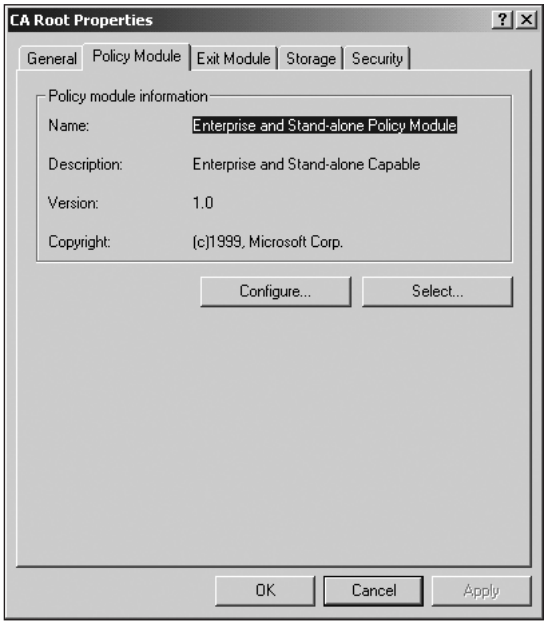

Figure 10-11 Policy Module page of CA object

The Configure button opens a separate dialog box with options for controlling the installed policy module. This dialog box has two pages:

- The Default Action page provides control over the processing of incoming requests. You can configure the CA to always issue a certificate when it receives a request or to mark the request as pending so that you can approve it manually.
- The X.509 Extensions page lets you edit a list of locations where CRLs are published and a list that specifies locations where users can retrieve the CA's certificate.

Exit Module Properties

The Exit Module page, shown in Figure 10-12, displays any exit modules configured for the CA. Exit modules define what happens after a certificate is issued. Only the default exit module, Enterprise and Stand-alone Exit Module, is available in Windows 2000. You can configure additional exit modules if you have them. The Configure button opens a separate dialog box that lets you control whether certificates are published in the Active Directory and in a local file system location.

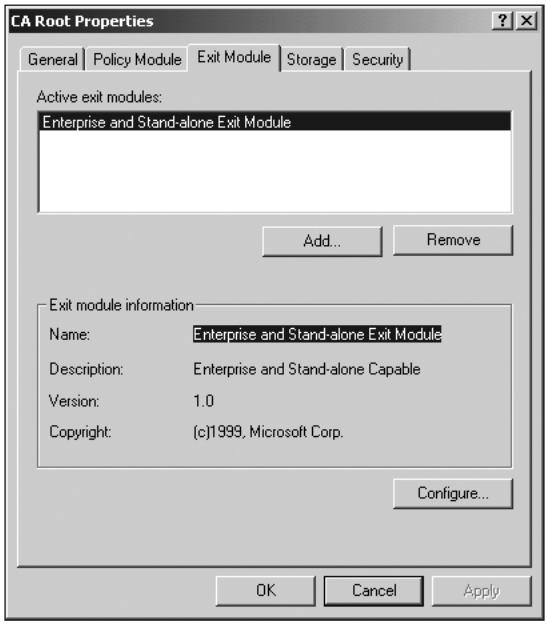

Figure 10-12 Exit Module page of the CA object

Storage Properties

The Storage page, shown in Figure 10-13, displays the paths where the CA keeps its configuration information and certificate database files. You cannot change these values once you install the CA, however. The Active Directory option lets you move the information on a Stand-alone CA with Active Directory access into the directory.

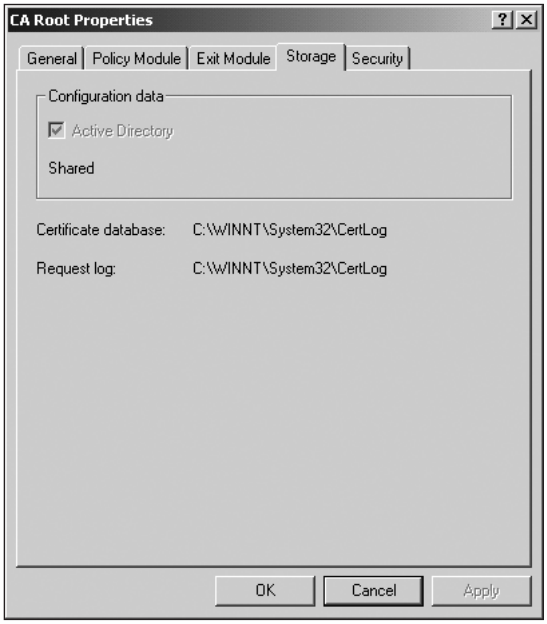

Figure 10-13 Storage page of CA object

Security Properties

The Security page looks like most other Security pages you see on objects in the Active Directory and allows you to assign access permissions on the CA object. Table 10-2 shows the permissions available for the CA object.

Table 10-2 Permissions available on the CA object

Permission	Description
Manage	Lets users change anything on the CA; granting this permission also grants all other permissions
Enroll	Lets users request new certificates for users or computers
Read	Lets users read certificates from the database
Write configuration	Lets users save CA configuration changes
Read configuration	Lets users read CA configuration data
Read control	Lets users read control information for the CA
Delete	Lets users remove objects from the CA database
Modify permissions	Lets users modify permissions on the CA object
Modify owner	Lets users modify ownership of CA objects
Revoke certificate	Lets users revoke certificates
Approve certificate	Lets users approve certificates marked as pending
Read database	Lets users read certificate information from the database

Certificate Enrollment

When a client obtains a certificate from a CA, this is called **certificate enrollment**. Windows 2000 provides two ways for a client to obtain a certificate.

Requesting a Certificate Using the Certificates Snap-in

The first way for a user to request a certificate is to use the Certificates snap-in shown in Figure 10-14.

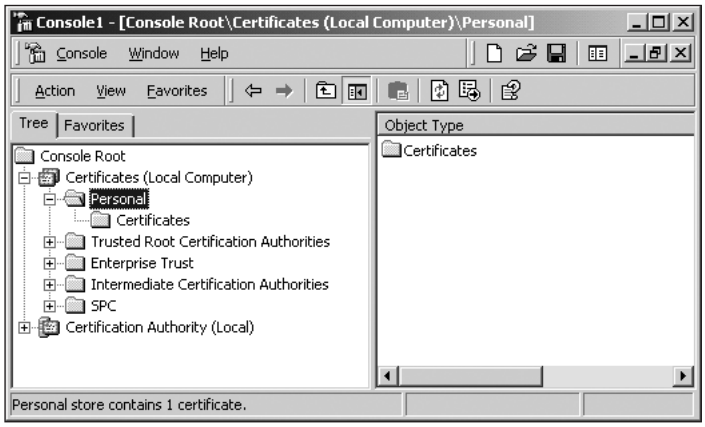

Figure 10-14 Using the Certificates snap-in

Just right-click the Personal folder and choose the Request New Certificate command from the All Tasks submenu. This starts a Certificate Request wizard that guides you through the process. Hands-on Project 10-3 at the end of the chapter outlines the steps for requesting a new certificate. The basic steps you follow are selecting a template for the certificate, selecting a particular CSP and CA if you want, and entering a friendly name for the certificate to help you remember its purpose.

Web Enrollment

If you chose to install the Web enrollment component of the CA during its initial setup, your CA also supports Web-based certificate requests from clients. By default, users can access the Web enrollment page using the URL http://*ca-name*/certsrv. On that page, users have three options:

- *Retrieve the CA Certificate or Certificate Revocation List button*: opens a set of pages for examining the certificate of the CA itself, the CRL, or the whole certification chain all the way to the root CA.
- *Request a certificate button*: leads you through a set of Web pages that simulate the wizard used to request a new certificate in the Certificates snap-in. For the most part, the settings are all the same. One difference is that the Web interface allows

you to supply the CA with a certificate request generated by another program in PKCS#10 format.

- *Check on a pending certification button*: looks up any pending requests and tells you whether they have been approved or not.

Managing Revocation

Generally, certificates are fairly long-lived. In fact, the default life of a new certificate issued by MCS is two years. When a certificate becomes untrustworthy prior to its expiration (such as through a security compromise or change in the subject's situation), you can revoke the certificate. Do not take this action lightly, however; revocation is a permanent action.

You can revoke any certificates issued by the CA you are managing by right-clicking the certificate in the Certification Authority snap-in and selecting the Revoke Certificate command from the All Tasks submenu. A dialog box opens that lets you mark a reason for the revocation—the default reason is "unspecified." Hands-on Project 10-4 at the end of the chapter outlines the steps for revoking a certificate.

As soon as you revoke a certificate, it is added to a Certificate Revocation List (CRL) for the server. The Revoked Certificates folder of the Certification Authority snap-in displays the certificates on this list. CAs publish CRLs containing revoked certificates for downloading or online viewing by client applications so that users can determine the status of certificates.

Removing Encrypting File System (EFS) Recovery Keys

Windows 2000 used the **Encrypting File System (EFS)** protocol to encrypt data on a computer by combining the data in those files with the public key certificate of the user logged on to the computer. Once encrypted, only that user's private key can be used to decrypt the files. In fact, the whole process is invisible to the user. From the user's perspective, encrypted folders appear normal and all the documents in them can be used normally. Access is denied to any other user attempting to view the contents of the folder. If access is somehow obtained, only encrypted information is presented.

Consult your Windows 2000 Professional or Windows 2000 Server documentation for details on how to encrypt and decrypt data.

For encrypted data, Windows 2000 creates a private encryption key for the file that it uses to encode the data. Then it creates a public encryption key to encrypt the private key. This is commonly referred to as lock-box security. In addition, the process generates a spare private encryption key called the **EFS Recovery Key** that can decrypt the data and then map that key to a trusted account called a **Recovery Agent**. By default, the administrator of a computer is designated the Recovery Agent. Removing this spare key provides an extra level of security, in that only the person with access to the original private key can decrypt the data. Hands-on Project 10-5 at the end of the chapter outlines the steps for removing the EFS Recovery Key.

Chapter Summary

- Windows 2000 incorporates a component named Microsoft Certificate Server (MCS) as part of a system to help ensure the accuracy and privacy of data as it is transferred over the network. MCS issues and manages certificates in an organization. Certificates provide two basic services to an organization: privacy, in the form of encrypting data; and authentication.
- MCS works using public key encryption, in which two separate keys—a public key and a private key—form a key pair to encrypt and decrypt data. Certificates are also used to allow verification of the claim that a given public key actually belongs to a given individual. The issuer of a certificate is called a Certificate Authority (CA).
- MCS acts as a CA for Windows 2000. MCS includes two policy modules that permit two different classes of CAs: Enterprise CAs and Stand-alone CAs. Within each class, Enterprise and Stand-alone, a CA can operate as either a root CA or a subordinate CA.
- Once installed in Windows 2000, the MCS component is managed using two snap-ins: the Certification Authority snap-in and the Certificates snap-in. Primary management tasks include certificate enrollment, renewal, and revocation.

Key Terms

Certificate Authority (CA) — Any trusted source willing to verify the identities of people to whom it issues certificates and to associate those people with certain public and private keys.

certificate enrollment — Process whereby a client obtains a certificate from a certificate authority.

Certificate Revocation Lists (CRL) — List of revoked certificates and the codes defining the reasons for revocation.

certificates — Allow verification of the claim that a given public key actually belongs to a given individual. This helps prevent an impersonator from using a phony key.

Certificate Store — Database created during the installation of a CA. Installing certificate services on an Enterprise root CA, creates the store in the Active Directory. Installing services on a Stand-alone root CA creates the store on the local server.

Certificate Trust List (CTL) — Holds the set of all root CAs whose certificates users and computers can trust.

EFS Recovery Key — Spare private encryption key capable of decrypting the data. The key maps to a trusted account called a Recovery Agent.

Encrypting File System (EFS) — Protocol Windows 2000 uses to encrypt data on a computer by combining the data in those files with the public key certificate of the user logged on to the computer.

Enterprise CA — Acts as a CA for an enterprise and requires access to the Active Directory.

Microsoft Certificate Server (MCS) — Windows 2000 component that acts as an authority for issuing and managing certificates.

pre-shared key — Single key used both to encrypt and decrypt data. This key is often a simple password shared beforehand by both the encrypting and decrypting parties.

private key — Part of a public/private key pair kept secret; the private key is only available to the person who holds the key.

public key — Part of a public/private key pair made publicly available.

public key encryption — Encryption method in which a recipient's public key encrypts data and then that same recipient's key decrypts the data.

public key infrastructure (PKI) — System of components working together to verify the identity of users who transfer data on a system and to encrypt that data if needed.

Recovery Agent — User designated as able to access the EFS Recovery Keys on a computer. By default, this is the administrator.

Rivest-Shamir-Adleman (RSA) algorithm — Most common public key encryption algorithm in use today, and the MCS default.

root CA — CA at the top of a CA hierarchy and trusted unconditionally by a client.

subordinate CA — CA beneath the root CA in the CA hierarchy and perhaps even under other subordinate CAs. Subordinate CAs typically issue certificates to users and computers in the organization.

Stand-alone CA — Used to issue certificates to users outside the enterprise and does not require access to the Active Directory.

X.509 certificate — Most widely used format for certificates, as defined by the International Telecommunications Union (ITU) in Recommendation X.509.

Review Questions

1. Which of the following keys form a key pair used to encrypt and decrypt data? (Choose two.)
   a. Private key
   b. Secret key
   c. Public key
   d. Shared key
2. What is the default encryption algorithm used by Windows 2000?
   a. Kerberos
   b. DEC
   c. RSA
   d. MD-5

3. Which of the following constructs verifies the identity of a person associated with a public key?
   a. Certificates
   b. Private Key
   c. Trust
   d. Certificate authority
4. A _____ is at the top of the CA hierarchy, and all clients in an organization can trust it.
5. A Stand-alone CA requires Active Directory access. True or false?
6. Which of the following are requirements for installing an Enterprise Root CA? (Choose all that apply.)
   a. Windows 2000 DNS Service
   b. Windows 2000 Active Directory Service
   c. Windows 2000 WINS Service
   d. Windows 2000 Routing and Remote Access Service
7. A Stand-alone subordinate CA requires a parent CA that is in the same domain. True or false?
8. Which of the following is the default hash algorithm used for computing digital signatures?
   a. MD-4
   b. MD-5
   c. SHA-1
   d. RSA
9. Which of the following permissions would you assign to a user on the CA object to allow that user to handle pending certificate requests?
   a. Modify certificate
   b. Approve certificate
   c. Write configuration
   d. Enroll
10. You cannot store multiple backups of a CA in the same folder using the CA Backup Wizard. True or false?
11. A _____ is the database used to hold certificates issued by a CA.
12. Which of the following actions does the Web enrollment feature of MCS allow you to do? (Choose all that apply.)
    a. View a certificate revocation list.
    b. Request a certificate.
    c. Renew a certificate.
    d. Remove a pending request that you generated, as long as it has not already been approved or denied.

13. _____ is a protocol used by Windows 2000 to encrypt data by combining the data in those files with the public key certificate of the user logged on to the computer.
14. What is the primary concern when renewing a CA's certificate by binding a new certificate to existing keys?
15. Assigning a user the _____ permission on a CA object automatically assigns the user all other permissions as well.
16. Which of the following standards is most commonly used for formatting certificates?
    a. X.25
    b. X.500
    c. X.506
    d. X.509
17. The _____ property page of the CA object is used to control which actions are performed after a certificate is issued.
18. A CA can store no more than 150,000 certificates in its database. True or false?
19. By default, which of the following users is designated the Recovery Agent and given a spare copy of the EFS Recovery Key used to encrypt a particular folder?
    a. The folder's owner
    b. The user who encrypted the folder
    c. The administrator
    d. Any user in the local Administrators group
20. A root CA must always renew its own certificates. True or false?

HANDS-ON PROJECTS

All Hands-on Projects in this chapter require at least one server computer set up as described in the lab set-up section in the front of this book.

Project 10-1

In this procedure, you install Microsoft Certificate Server as an Enterprise Root CA. To do this, your computer must have access to Active Directory and DNS services, and you must have enterprise Administrator privileges on the DNS and Active Directory. You must also have Administrator privileges on the local server.

To install Microsoft Certificate Server on a local computer:

1. Click **Start**, point to **Settings**, and then click **Control Panel.**
2. Double-click the **Add/Remove Programs** icon.
3. In the dialog box that opens, click the **Add/Remove Windows Components** button.

4. When the Windows Components Wizard starts, select **Certificate Services** from the list of components.

   You should see a warning that once you install the services, you cannot rename the computer, nor can it join or leave a domain.
5. Click **Yes** to continue.
6. Click the **Next** button.
7. Make sure that the **Enterprise root CA** option is selected, and click **Next** to continue.
8. On the **CA Identifying Information** page, enter the information appropriate to your CA, then click the **Next** button.
9. Note the locations of the database and database logs, and click the **Next** button.
10. If Internet Information Services is running on the computer, the wizard needs to stop the services. Click **OK** to allow the wizard to proceed.
11. The wizard begins copying necessary files. It may prompt you for the location of the Windows 2000 set-up files and any files for service packs that have been installed. When the wizard finishes, click **Finish** to exit.

Project 10-2

To create a new MMC console and add the Certification Authority and Certificates snap-ins:

1. Click **Start** and then click **Run**.
2. In the Run field, type **mmc** and then click the **OK** button.
3. From the Console menu, select the **Add/Remove snap-in** command.
4. In the Add/Remove snap-in dialog box, click the **Add** button.
5. From the list of available snap-ins, select the Certification Authority snap-in and click the **Add** button.
6. In the Certification Authority dialog box that opens, make sure **Local computer** is selected and click **Finish**. If you want to manage another computer (say you want to manage the CA server from your workstation), select the Another computer option and enter the computername. Then return to the Add Stand-Alone Snap-In dialog box.
7. Select the **Certificates snap-in** from the list, and click the **Add** button.
8. In the Certificates Snap-In dialog box, choose **Computer Account** and then click **Next**.
9. Make sure the Local option is selected and click **Finish**.
10. Click **OK** to return to the new console.
11. The new console should now show both snap-ins. Make sure to save the console so that you do not have to re-create it later.

Project 10-3

To request a new certificate:

1. In the Certificates snap-in, right-click the **Personal** folder and choose the **Request New Certificate** command from the All Tasks submenu.
2. On the introductory page of the wizard, click **Next** to go on.
3. The next page of the wizard lists all available templates that you can access. The list's content depends on the permissions set up for templates in your domain. Make sure the default is selected, and click **Next**. If you select the **Advanced** option, the wizard presents two additional steps covered in Steps 4 and 5.
4. If you selected the **Advanced** option in Step 3, the next page you see lets you choose a Cryptographic Service Provider, if one in addition to the default Windows 2000 option is available. Click **Next**.
5. If you selected the **Advanced** option, you also see a wizard page where you can choose the specific CA and computer to which your request is sent. Click **Next**.
6. The next page you see (whether or not you chose to view advanced options) lets you enter a friendly name and description for the certificate. Type a **name** and **description** that helps you remember the certificate's purpose, and click **Next**.
7. The final page summarizes your choices. Click **Finish** to complete your request. Depending on the CA's setup, you may get an immediate response or have to wait for an administrator's approval.

Project 10-4

To revoke a certificate:

1. In the Certification Authority snap-in, expand the Certificate Authority that issued the certificate you want to revoke.
2. Select the **Issued Certificates** folder in the left pane.
3. In the right pane, right-click the certificate you want to revoke and choose the **Revoke Certificate** command from the **All Tasks** submenu.
4. Select a **reason code** for the revocation, and click **Yes**.

Project 10-5

To remove an EFS Recovery Key:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Local Security Policy**.
2. Expand the **Public Key Policies** container, and select the **Encrypted Data Recovery Agents** container inside.
3. Right-click **an agent** in the right pane, and select **Delete Policy** from the shortcut menu.
4. A warning dialog appears asking you to confirm the deletion. Click **Yes** to continue.

If you want, you can right-click the agent and select the Export command to copy the recovery key to a floppy disk before removing it from the Local Security Policy. Since you can fit many such keys on a single floppy disk, this provides a way to create a master key disk of sorts.

CASE PROJECTS

Case 1

You are the administrator of a large network and need to set up secure access to information on your extranet for your customers as well as for the internal users on your network. You decide to purchase services from VeriSign, an external CA, so that you do not have to validate your customers' identities yourself. You have also decided to set up Certificate Services within your own organization to help ease the burden of certification traffic from your internal users. Outline the steps you will take to set up these services.

Case 2

Your security needs change and you decide to reconfigure the PKI on your network to not use any external CA. Your organization consists of a single Active Directory Forest and one domain tree that contains six domains. You want to set up a CA in each domain, but configure one central CA to be the most trusted in the organization. Sketch the CA hierarchy you will use and indicate the class and role of each CA in that hierarchy.